Sub B2

~~36. The method of claim 28 wherein the network events include monitoring network~~ connections by monitoring a correlation of network connection requests and network connection denials.

37. The method of claim 28 wherein the network events include monitoring errors by monitoring error codes included in a network packet.

38. The method of claim 28 wherein the network events include monitoring errors by monitoring network packet privilege codes.

39. The method of claim 28 wherein the integrating comprises:
filtering network events; and
summarizing network events.

40. The method of claim 28 wherein the correlating comprises:
filtering the integrated network events; and
summarizing the network events.

Sub B3

41. The method of claim 28 further comprising:
distributing the correlated network events via a link to subscribers.

42. The method of claim 41 wherein the link is a secured link.

43. The method of claim 41 wherein the distributing comprises sending the correlated network events via electronic mail.

44. The method of claim 41 wherein the subscribers are the service monitors

45. The method of claim 41 wherein the subscribers are the domain monitors.

a Cont.

46. The method of claim 44 further comprising:
filtering the received correlated network events in the service monitors; and
summarizing the received filtered correlated network events in the service monitors.

Sub B3

47. The method of claim 44 further comprising:
filtering the received correlated network events in the domain monitors; and
summarizing the received filtered correlated network events monitors.

48. A method of hierarchical event monitoring and analysis within an enterprise network comprising:
~~deploying hierarchical network monitors in the enterprise network;~~

Sub B2

~~detecting, by the hierarchical network monitors, suspicious network activity based~~ on analysis of network traffic;

generating, by the hierarchical network monitors, reports of the suspicious activity; and

automatically receiving and integrating the reports of suspicious activity, by one or more hierarchical network monitors.

49. The method of claim 48 wherein the hierarchical networks monitors are located in domains of the enterprise network.

50. The method of claim 48 wherein the analysis of network traffic comprises monitoring data transfer errors.

51. The method of claim 48 wherein the analysis of network traffic comprises monitoring data transfer volume.

Sub B2

B

52. The method of claim 48 wherein the analysis of network traffic comprises monitoring network connection requests.

53. The method of claim 48 wherein the analysis of network traffic comprises monitoring network connection denials.

54. The method of claim 48 wherein the analysis of network traffic comprises monitoring a correlation of network connection requests and network connection denials.

55. The method of claim 48 wherein the analysis of network traffic comprises monitoring rejected packet error codes.

56. The method of claim 48 wherein the analysis of network traffic comprises monitoring privilege error codes.

a3 cont.

57. The method of claim 48 wherein generating reports comprises:

filtering the suspicious network activity; and

summarizing the filtered suspicious network activity.

Sub B3

58. The method of claim 49 wherein receiving and integrating the reports of suspicious activity is performed in domain network monitors associated with sets of network monitors.

59. The method of claim 58 wherein the domain network monitors are associated with ~~an enterprise network monitor~~.

~~60. The method of claim 58 wherein integrating the reports is performed in the~~ domain monitors.

Sub B2

61. The method of claim 59 wherein integrating the reports is performed in the enterprise network monitor.

62. The method of claim 61 wherein the integrating comprises:
correlating the suspicious network activity based on commonalities.

63. The method of claim 62 further comprising:
invoking countermeasures to the integrated reports of suspicious network activity

A2 concl.

64. The method of claim 48 wherein the network monitors include an application program interface (API) for encapsulation of monitor functions and integration of third party tools.

Sub B2

65. The method of claim 48 wherein the enterprise network is a TCP/IP network.

66. The method of claim 48 wherein the network monitors are deployed in gateways.

67. The method of claim 48 wherein the network monitors are deployed in routers.

68. The method of claim 48 wherein the network monitors are deployed in proxy ~~servers.~~

In the Abstract:

On page 37, delete lines 1-8 and insert:

-- A method of hierarchical event monitoring and analysis within an enterprise network including deploying hierarchical network monitors in the enterprise network, detecting, by the hierarchical network monitors, suspicious network activity based on analysis of network traffic, generating, by the hierarchical network monitors, reports of the suspicious activity and automatically receiving and integrating the reports of suspicious activity, by one or more hierarchical network monitors.--

A3

Sub B3

REMARKS

Applicants submit this preliminary amendment in the filing of a 37 C.F.R. 1.53(b) continuation.